CAPINCROUSE LLP

Is Your Organization Managing Risk – or is Risk Managing You?

By Fran Brown, Managing Partner

All entities make decisions based on risk every day. That means Enterprise Risk Management (ERM) is a process that all higher education institutions, churches, schools, and ministries are already implementing. The question is: Is your organization managing the ERM process — or do you just react to risk after the fact?

How Your Organization Can Benefit from ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as:

> …a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

A properly designed and implemented ERM process will help your organization align risk and strategy, enhance your risk response decisions, and reduce operational surprises and losses. As noted above, all entities make decisions based on risk every day. The key is how your organization is managing that risk and what data you are using to make the best decisions.

A properly functioning ERM process will also allow your organization to identify and manage multiple and cross-enterprise risks, seize opportunities, and properly deploy capital. It's important to note that ERM is not a risk avoidance process — it is a risk understanding process that allows for better decisions.

How to Implement an Effective ERM Strategy

ERM is best organized across four broad categories to achieve your objectives:

- Strategic
- Operations
- Reporting
- Compliance

The administration of ERM focuses on eight interrelated components that bring in data and resources from the four broad categories above. When an organization implements the ERM process, it looks across the:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control objectives
- Information and communication
- Monitoring

We recommend using a three-phase approach to creating an ERM strategy.

Phase One: Data Gathering and Training

1. Survey or interview employees about perceived risks. The information gathered during this step establishes a framework for what is perceived as risks at different levels across the organization.
2. Train key individuals on how to identify and manage the risk associated with the different items identified. This training is important to help key individuals understand what to look for, as well as ways to mitigate the risk.

Phase Two: Identification and Assessment

1. Identify and classify the risks based on the likelihood of each event occurring, as well as the impact such an event would have. For instance, a slip and fall on your property could be likely in the winter months (for those of us who suffer through the cold), but the impact would be relatively small. A data breach of critical student or donor information may be less likely, but the impact would be significantly larger.
2. Prioritize your list. After all the data has been gathered and all the risks have been measured, we recommend that you narrow the list down to no more than 15 risks. If you include more than 15, you may end up spread too thin or focused on risks that are not

likely to happen and would not be impactful even if they did occur.

3. Assign responsibility for each risk to someone within the organization.
4. Execute a plan of action for each risk. In the example of the slip and fall risk, you may just need to make sure the proper insurance is in place. To address the risk of a potential data breach, an IT audit may be necessary.

Phase Three: Reporting and Monitoring

1. Create and implement a system for reporting the process around each risk. This system must allow for the risk to be monitored, mitigated, and reported upon at regular intervals.
2. Monitor and address risks as needed. This is where you may have a risk drop out of your top 15 and a new risk rise to replace it.

It is important to note that ERM does not end with phase three, however. ERM is a process and must be continuously monitored, updated, and reported on. All departments should have representation within the process, and each risk should have an owner. This will keep ERM a moving and evolving process.

The ERM process can seem overwhelming, but CapinCrouse can assist your organization in educating, defining, and implementing the ERM process. We can help you through each phase, including surveying employees, organizing and analyzing the data, identifying and prioritizing risks, and implementing an effective system tailored to your organization's needs. Please contact us if you are interested in learning more about how we can serve your organization in this area.

About the Author

Fran Brown, Managing Partner
fbrown@capincrouse.com
o 617.535.7534

As Managing Partner, Fran leads the firm and guides the implementation of strategic plans and objectives. He is also involved in client acquisition meetings, significant board meetings, and representing the firm nationally. Fran has more than 30 years of experience providing audit and management consulting services to a variety of nonprofit entities, including colleges and universities. Fran previously led the New England Higher Education and Not-for-Profit Practice at Grant Thornton and was partner-in-charge of the not-for-profit practice at CCR LLP. His expertise includes strategic planning, budgeting, financial statement preparation, exempt-organization tax filing, real property sales and leases, board training, and enterprise risk management (ERM) training.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

© Copyright 2016 CapinCrouse LLP

ERM is not a risk avoidance process — it is a risk understanding process that allows for better decisions.